eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Scanners**
  - ✓ Conhecendo o Nikto
    - ✓ Características do Nikto
    - ✓ Principal opção de uso
    - ✓ Opções complementares
    - ✓ Opções de formatos de relatórios
    - ✓ Opções de Tuning
  - ✓ Conhecendo Nessus
    - ✓ Instalando Nessus
  - ✓ Conhecendo Acunetix
    - ✓ Instalando Acunetix

Vuln Scanner: Nikto

Nikto é um web scanner Open Source (GPL), que realiza testes abrangentes contra servidores web com vários itens, incluindo uma lista com mais de 6700 arquivos/programas potencialmente perigosos.

Verifica a existência de versões desatualizadas de mais de 1.250 serviços e problemas específicos de versão.

Ele também verifica a existência de itens de configuração do servidor, como a presença de vários arquivos de índice, opções do servidor HTTP, e tentará identificar os serviços web instalados e softwares.

Itens de scanner e plugins são atualizados com frequência e podem ser atualizados automaticamente.

Vuln Scanner: Nikto

Nikto não foi concebido como uma ferramenta furtiva.

Ela irá testar um servidor web no menor tempo possível, e é óbvio que decorrente disto, torna-se muito barulhenta para um IPS / IDS. No entanto, não há suporte para métodos anti-IDS de libwhisker no caso de você querer experimentá-lo (ou testar o seu sistema IDS).

Nem todo teste é um problema de segurança, embora a maioria são.

O itens de vulnerabilidades do tipo “info” são normalmente marcados apropriadamente na informação impressa.

Há também algumas verificações para os itens desconhecidos que foram scaneanos em arquivos de log.

Vuln Scanner: Nikto

Aqui estão algumas das principais características do Nikto:

- SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's
- Perl/NetSSL)
- Full HTTP proxy support
- Checks for outdated server components
- Save reports in plain text, XML, HTML, NBE or CSV
- Template engine to easily customize reports
- Scan multiple ports on a server, or multiple servers via input file (including nmap output)
- LibWhisker's IDS encoding techniques
- Easily updated via command line
- Identifies installed software via headers, favicons and files
- Host authentication with Basic and NTLM
- Subdomain guessing
- Apache and cgiwrap username enumeration
- Mutation techniques to "fish" for content on web servers

Vuln Scanner: Nikto

- Scan tuning to include or exclude entire classes of vulnerability
- checks
- Guess credentials for authorization realms (including many default id/pw combos)
- Authorization guessing handles any directory, not just the root
- directory
- Enhanced false positive reduction via multiple methods: headers,
- page content, and content hashing
- Reports "unusual" headers seen
- Interactive status, pause and changes to verbosity settings
- Save full request/response for positive tests
- Replay saved positive requests
- Maximum execution time per target
- Auto-pause at a specified time
- Checks for common "parking" sites
- Logging to Metasploit
- Thorough documentation

Vuln Scanner: Nikto

Modo de uso:

Execute o Nikto de forma simples com as opções –h (host) e –o (Output):
niktop –h www.alvo.com –o report.html

Veja algumas opções interessantes:
-noSSL – Não efetua varreduras usando SSL (HTTPS)
-id – Efetua varreduras em páginas com credenciais. Ex: nikto –id usuario:senha
-ssl – Força o uso da porta SSL
-timeout – Seta a espera em segundos caso o servidor demora à responder (padrão 2 segundos)
-update – Efetua a atualização da base de dados do Nikto
-version – Apresenta a atual versão utilizada
-port – Você pode setar uma porta diferente (Padrão 80)
-userproxy – Processo de evasão do Nikto. Ex: nikto –useproxy http://10.0.0.1:8080
-findonly – Faz uma pequena varredura sobre o ambiente mas não procura por falhas. Verifica as portas e busca por headers apenas.

Vuln Scanner: Nikto

-format – Junto com a opção –o, gera relatório em diversos formatos (csv, txt, html e xml)

-mutate – Especifica o método de varredura.

1 – Testa todos os arquivos no diretório principal
2 – Procura por arquivos que contém senhas
3 – Enumera usuários do apache (/~user)
4 – Enumera usuários via CGIWRAP (/cgi-bin/cgi-wrap/~user)
5 – Efetua brute force em busca de Subdominios e Hostname
6 – Efetua brute force em busca de diretórios e subdiretórios

-mudate-options – Especifica opções da função mutate, por exemplo arquivo para brute force: -mudate 5 –mutate-options /bruteforce.txt

-plugins – Seleciona um plugin específico (para ver a lista de plug-ins, use a opção –plugins-list)

-pause – Seta o intervalo de tempo entre cara teste de vulnerabilidade

-vhost – Especifica o Host header ao alvo, muito utilizado em servidores que possuem diversos sites

Vuln Scanner: Nikto

-tuning – Este ajuste vai controlar que tipo de teste o Nikto irá realizar.
Por padrão, apenas testes de vulnerabilidades serão executados, porém, você pode alterar esse parâmetro para que ele efetue o ataque juntamente com o teste.

- 0 – File Upload
- 1 – Busca por arquivos interessantes
- 2 – Erros de configuração
- 3 – Divulgação de informações
- 4 – Injection (XSS, Script e HTML)
- 5 – Recuperação de arquivos remotos (apenas na raíz)
- 6 – Denial of Service
- 7 – Remote file retrieval (em todo servidor)
- 8 – Execução de Comando / Shell remota
- 9 – SQL Injection
- a – Bypass de autenticação
- b – Identificação de Software
- c – Inclusão de Código Remoto
- x – Opções reversas do Tuning (Inclui todos, exceto especificado aqui)

Vuln Scanner: Nessus

Nessus é um programa de verificação de falhas/vulnerabilidades de segurança. Ele é composto por um cliente e servidor, sendo que o scan propriamente dito é feito pelo servidor.

O nessusd (servidor Nessus) faz um port scan ao computador alvo, depois disso vários scripts (escritos em NASL, Nessus Attack Scripting Language) ligam-se a cada porta aberta para verificar problemas de segurança.

Vuln Scanner: Nessus

Instalando:

Baixe o instalador de acordo com seu sistema operacional e arquitetura
http://www.tenable.com/products/nessus/select-your-operating-system

Execute a instalação com o comando abaixo:
dpkg –i Nessus-5.2.2-debian6_amd64.deb

Após esse processo, inicie o serviço através do comando abaixo:
/etc/init.d/nessusd start

Por ultimo, acesse o Nessus através do link abaixo e conclua a instalação:
https://127.0.0.1:8834/

Vuln Scanner: Acunetix

Vuln Scanner: Acunetix

O Acunetix é sem dúvida alguma o scanner web mais utilizado por hackers, administradores de sites, webmasters e analistas de segurança.

Com esse scanner você consegue fazer uma varredura completa em um site em busca de vulnerabilidades.

Todo o processo de scanning é automatizado, você precisa apenas informar o endereço do site alvo ou ip do mesmo e escolher para quais vulnerabilidades você quer que o Acunetix execute no site alvo.

printf ("\Chega por hoje\n");

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker